LANCOM SYSTEMS

Whitepaper

Ist VPN als Verschlüsselungstechnologie für das Post-Quantum-Zeitalter noch sicher genug?

Die fortschreitende Entwicklung von Quantencomputern stellt traditionelle Verschlüsselungstechnologien wie VPN vor grundlegende Herausforderungen. Virtual Private Networks (VPNs), die oft auf dem Internet Key Exchange (IKE)-Protokoll basieren, bilden das Rückgrat vieler moderner IT-Sicherheitslösungen. Doch wie sicher ist diese Technologie angesichts der wachsenden Bedrohung durch Quantencomputer?

Ein erster Schritt zur Absicherung gegen die Bedrohungen durch Quantencomputer ist die Einführung von Post-Quantum Preshared Keys (PQ-PSKs oder PPK) im IKEv2-Protokoll. Diese Technologie bietet eine vielversprechende Grundlage, um VPNs zukunftssicher zu gestalten und potenziellen Angriffen durch Quantencomputer frühzeitig entgegenzuwirken.

Strategie von LANCOM Systems für das Post-Quantum-Zeitalter

LANCOM Systems verfolgt eine zukunftsorientierte Strategie, um seine Produkte und Lösungen frühzeitig auf die Bedrohungen des Post-Quantum-Zeitalters vorzubereiten. Ziel ist es, Unternehmen, Behörden und Betreibern Kritischer Infrastrukturen einen sicheren Übergang in eine Ära zu ermöglichen, in der Quantencomputer asymmetrische Verschlüsselungsverfahren gefährden könnten.

Proaktive Vorbereitung und Einhaltung von Standards

LANCOM Systems folgt den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Einführung von Post-Quanten-Kryptografie, wie in der Erklärung des BSI im November 2024[1)] beschrieben.

Das Unternehmen setzt auf eine schrittweise und praxisorientierte Integration von Post-Quantum-Sicherheitsmechanismen in seine Produktpalette, um Kunden einen nachhaltigen und sicheren Übergang zu ermöglichen.

Einführung von Post-Quantum Preshared Keys

Ein zentraler Bestandteil dieser Strategie ist die Einführung von Post-Quantum Preshared Keys (PQ-PSKs) im IKEv2-Protokoll. Diese Technologie wird ab 2025 mit LCOS 10.90 verfügbar sein und bietet eine erste Schutzmaßnahme gegen potenzielle Angriffe durch Quantencomputer.

Ausbau der Post-Quantum-Funktionalitäten

Im weiteren Verlauf des Jahres 2025 wird LANCOM Systems die Post-Quantum-Funktionalitäten weiter ausbauen. Mit LCOS FX 11.3 und der Implementierung von

1) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html?nn=129156#Download=1

ML-KEM wird eine noch robustere Sicherheitsarchitektur bereitgestellt, die den neuesten Erkenntnissen in der Post-Quanten-Kryptografie entspricht.

Quantencomputing und die Bedrohung für klassische Verschlüsselung

Warum Quantencomputer herkömmliche Kryptografie gefährden

Quantencomputer nutzen die Gesetze der Quantenmechanik, um komplexe Berechnungen in kürzester Zeit durchzuführen. Sie sind in der Lage, zwei fundamentale kryptografische Säulen zu brechen:

1. **Asymmetrische Verschlüsselung**: Algorithmen wie RSA und Elliptic Curve Cryptography (ECC) basieren auf mathematischen Problemen, die von Quanten-algorithmen wie Shor‘s Algorithmus effizient gelöst werden können.
2. **Symmetrische Verschlüsselung**: Auch symmetrische Algorithmen wie AES werden durch Quantencomputer beeinträchtigt, obwohl der Schaden hier weniger gravierend ist (z. B. durch Grover‘s Algorithmus).

Auswirkungen auf VPNs

VPNs, die IKEv2 als Schlüsselaustauschprotokoll nutzen, verwenden asymmetrische Kryptografie, um Sitzungsschlüssel sicher auszutauschen. Diese Schlüssel könnten von Quantencomputern in Zukunft kompromittiert werden, wodurch alle verschlüsselten Daten offengelegt werden könnten – auch rückwirkend.

Post-Quantum Preshared Keys (PQ-PSKs): Die Lösung

Wie PQ-PSKs funktionieren

Post-Quantum Preshared Keys (PQ-PSKs) ergänzen herkömmliche kryptografische Mechanismen, indem sie eine zusätzliche, quantenresistente Sicherheitskomponente in den Schlüsselaustauschprozess integrieren. Hierbei wird ein vorab zwischen den Kommunikationspartnern geteilter Schlüssel (Preshared Key) verwendet, der unabhängig von asymmetrischen Algorithmen ist. Dieses Prinzip basiert auf dem Ansatz der hybriden Kryptografie: die Kombination traditioneller und quantensicherer Methoden, um die Sicherheitsstärken beider Ansätze zu vereinen.

1. **Zusätzliche Schutzschicht**
   Der PQ-PSK wird bei der Schlüsselaushandlung im IKEv2-Protokoll als zusätzlicher Authentifizierungs- und Verschlüsselungsfaktor eingeführt. Dadurch entsteht ein Sicherheitsmechanismus, der selbst dann intakt bleibt, wenn die klassische asymmetrische Kryptografie durch einen Quantenangriff gebrochen wird. Der PQ-PSK wird in den Prozess integriert, indem er in Kombination mit etablierten Verfahren (z. B. RSA oder ECC) verwendet wird, was den gesamten Schlüsselaustausch stärkt.

2. **Quantenresistenz durch robuste Algorithmen**
   PQ-PSKs setzen auf Algorithmen, die gegen Quantencomputer resistent sind. Diese Algorithmen basieren auf mathematischen Problemen, die auch für Quantencomputer schwierig zu lösen sind, wie beispielsweise:
   - **Gitterbasierte Kryptografie**: Sicherheit basiert auf der Schwierigkeit, kürzeste Vektoren in Gitterstrukturen zu finden.
   - **Code-basierte Kryptografie**: Nutzung fehlerkorrigierender Codes als Grundlage für Verschlüsselung.
   - **Mehrvariablen-Polynom-Systeme**: Probleme mit multiplen Variablen, die schwer zu berechnen sind.
3. **Vorab geteilter Schlüssel**
   Der Schlüssel wird außerhalb des regulären Schlüsselaustauschprozesses sicher bereitgestellt. Dies kann durch physische Übergabe, eine separate sichere Verbindung oder andere bewährte Verfahren erfolgen. Diese physische oder getrennte Verteilung sorgt dafür, dass der PQ-PSK nicht durch Angreifer abgefangen werden kann, selbst wenn der Datenverkehr selbst überwacht wird.
4. **Integrierte Sicherheitsprüfung**
   Während der Handshake-Phase im IKEv2-Protokoll prüft jede Partei die Gültigkeit des PQ-PSK. Dies schützt nicht nur vor zukünftigen Quantenangriffen, sondern auch vor aktuellen Angriffen wie Man-in-the-Middle-Attacken, bei denen ein Angreifer versucht, die Schlüsselaushandlung zu manipulieren.
5. **Rückwirkender Schutz**
   Ein besonders wichtiger Aspekt von PQ-PSKs ist der Schutz vor „Store-Now-Decrypt-Later"-Angriffen (SNDL). Bei diesen Angriffen speichern Angreifer verschlüsselte Daten, um sie zu entschlüsseln, sobald leistungsstarke Quantencomputer verfügbar sind. Durch die Verwendung von PQ-PSKs bleiben die gespeicherten Daten sicher, da sie ohne Zugriff auf den vorab geteilten Schlüssel nicht entschlüsselt werden können.
6. **Kompatibilität und Übergangsphasen**
   PQ-PSKs können in bestehende IKEv2-basierte VPN-Infrastrukturen integriert werden, ohne dass die asymmetrischen Verfahren vollständig ersetzt werden müssen. Diese hybride Vorgehensweise erleichtert die Implementierung und erlaubt es Organisationen, schrittweise in die neue Technologie zu investieren. So können klassische Systeme weiterhin genutzt werden, während gleichzeitig eine quantensichere Ebene hinzugefügt wird.

Vorteile von PQ-PSKs

→ Resistenz gegen Quantenangriffe: PQ-PSKs nutzen quantenresistente Algorithmen, die selbst mit leistungsstarken Quantencomputern nicht effizient geknackt werden können.

→ Nahtlose Integration: Die Technologie kann in bestehende IKEv2-basierte VPN-Infrastrukturen integriert werden, ohne dass grundlegende Änderungen erforderlich sind.

→ Langfristige Absicherung: Unternehmen können ihre Verschlüsselung bereits heute gegen zukünftige Bedrohungen sichern.

Praktische Anwendung und Implementierung

Einführung in bestehende Netzwerkinfrastrukturen

Die Einführung von Post-Quantum Preshared Keys ist besonders für Branchen und Szenarien relevant, in denen langfristige Vertraulichkeit und Datenintegrität von entscheidender Bedeutung sind. Hier einige Beispiele und der damit verbundene Handlungsbedarf.

1. Unternehmensnetzwerke

Unternehmen, die sensible Daten zwischen Standorten übertragen, wie Finanzdaten, interne Strategiepapiere oder personenbezogene Daten, stehen vor der Herausforderung, diese Informationen auch gegen zukünftige Bedrohungen zu schützen.

2. Kritische Infrastrukturen

Betreiber von Energie-, Wasser- und Verkehrsnetzen müssen sich gegen potenzielle Angriffe absichern, da deren Netzwerke für Angreifer besonders lukrativ sind.

3. Gesundheitswesen

Elektronische Patientenakten, medizinische Forschungsergebnisse und andere vertrauliche Informationen müssen geschützt werden, um Datenschutzrichtlinien wie die DSGVO zu erfüllen und das Vertrauen von Patienten zu sichern.

4. Finanzsektor

Banken und Finanzdienstleister verarbeiten große Mengen an Transaktionen und sensiblen Kundendaten, die langfristig geschützt werden müssen.

5. Behörden und öffentliche Verwaltung

Behörden speichern und übertragen Daten mit langfristiger Vertraulichkeit, beispielsweise Verschlusssachen, Bürgerdaten und strategische Planungen.

Die Handlungsbedarfe mögen sich in den verschiedenen Branchen unterscheiden, die praktische Umsetzung erfolgt jedoch in allen Fällen in zwei einfachen Schritten:

1. Firmware-Update

Bestehende VPN-Endpunkte müssen auf Firmware-Versionen aktualisiert werden, die PQ-PSKs unterstützen.

2. Konfiguration

Erweiterung einer bestehenden VPN-Verbindung der PQ-PSK.

Die konkrete Umsetzung von Schritt 2 in einer LANCOM Infrastruktur wird in diesem Knowledge Base-Artikel beschrieben:
https://knowledgebase.lancom-systems.de/display/KB/Erweiterung+einer+bestehenden+IKEv2-Verbindung+zwischen+zwei+LANCOM+Routern+mit+Post-quantum+Preshared-Keys

Zukunftssicherheit durch PQ-PSKs

Die Einführung von Post-Quantum Preshared Keys stellt einen wichtigen ersten Schritt dar, um VPNs für das Post-Quantum-Zeitalter zu rüsten. Obwohl Quantencomputer derzeit nicht in der Lage sind, klassische Verschlüsselung wie RSA oder ECC zu brechen, wird ihre Entwicklung aktiv vorangetrieben. Sobald leistungsstarke Quantencomputer verfügbar sind, könnten sie asymmetrische Verschlüsselungsalgorithmen relativ schnell kompromittieren. Daher ist es wichtig, nicht erst auf den technologischen Durchbruch von Quantencomputern zu warten, sondern schon jetzt mit der Absicherung von IT-Infrastrukturen zu beginnen.

Fazit

VPNs bleiben eine tragfähige Sicherheitslösung, wenn sie mit zukunftsweisenden Technologien wie PQ-PSKs ergänzt werden. Unternehmen, die frühzeitig auf diese Entwicklung setzen, verschaffen sich einen entscheidenden Vorteil in einer zunehmend unsicheren digitalen Welt. Die Investition in Post-Quantum-Technologien ist nicht nur eine Vorsichtsmaßnahme, sondern auch ein Ausdruck von Innovation und Weitsicht.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de